Notice of Allowability	Application No.	Applicant(s)	
	10/611,472	SZOR, PETER	
	Examiner	Art Unit	
	RONALD BAUM	2139	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to *12/3/2007*.

2. ☒ The allowed claim(s) is/are *1-16 and 19-33*.

3. ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
   a) ☐ All b) ☐ Some* c) ☐ None of the:
      1. ☐ Certified copies of the priority documents have been received.
      2. ☐ Certified copies of the priority documents have been received in Application No. _____ .
      3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

   * Certified copies not received: _____.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.
THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

4. ☐ A SUBSTITUTE OATH OR DECLARATION must be submitted. Note the attached EXAMINER'S AMENDMENT or NOTICE OF INFORMAL PATENT APPLICATION (PTO-152) which gives reason(s) why the oath or declaration is deficient.

5. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
   (a) ☐ including changes required by the Notice of Draftsperson's Patent Drawing Review (PTO-948) attached
      1) ☐ hereto or 2) ☐ to Paper No./Mail Date _____.
   (b) ☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____.

   Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).

6. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

1. ☒ Notice of References Cited (PTO-892)
2. ☐ Notice of Draftperson's Patent Drawing Review (PTO-948)
3. ☒ Information Disclosure Statements (PTO/SB/08), Paper No./Mail Date 20070820
4. ☐ Examiner's Comment Regarding Requirement for Deposit of Biological Material
5. ☐ Notice of Informal Patent Application
6. ☐ Interview Summary (PTO-413), Paper No./Mail Date _____ .
7. ☐ Examiner's Amendment/Comment
8. ☒ Examiner's Statement of Reasons for Allowance
9. ☐ Other _____.

DETAILED ACTION

Examiner's Statement of Reasons for Allowance

1. Claims 1-16, 19-33 are allowed over prior art.

2. This action is in reply to applicant's correspondence of 03 December 2007.

3. The following is an examiner's statement of reasons for the indication of allowable claimed subject matter.

4. As per claims 1, 5, 16 and 27-29 generally, prior art of record, Magdych et al, U.S. Patent No. 6,546,493 B1, and further in view of Hollander et al, U.S. Patent No. 6,412,071 B1, fails to teach alone, or in combination, at the time of the invention, the features as discussed and remarked upon in the response of 03 December 2007 to office action of 20 August 2007.

Specifically, (as per claim 1, for example) prior art dealing with the ability to scan and subsequently detect obfuscated polymorphic and metamorphic versions of malware via various anomaly and signature based algorithm analysis (i.e., detecting variants via the 'SAVE' algorithm utilizing similarity measures/metrics on executable code/system calls, inclusive of malware signature/behavior aspects; Sung, A.H., et al, 'Static Analyzer of Vicious Executables (SAVE)', IEEE, ACSAC 2004, entire document, http://ieeexplore.ieee.org/iel5/9473/30059/01377239.pdf?arnumber=1377239), is generally known per se. Nowhere in the prior art is found collectively the *italicized* claim elements (i.e., the specific aspects of signature extraction of [specific block/bytes] malware [executable] code, relative to the calling address location [backwards], with the subsequent forwarding to another processing [computer] system), at the ***time** of the invention*, serving to patently distinguish the invention from said prior art;

"1. A method comprising:

detecting an attack by

malicious code on

a first computer system;

***extracting** a malicious **code signature** from*

said *malicious code* comprising:

locating a caller's

***address** of said **malicious code** in*

***a memory** of said first computer system*; and

extracting

a specific number of bytes backward from** said **caller's address;

creating an *extracted malicious code packet including*

said malicious code signature; and

sending said *extracted malicious code packet* from

said first computer system *to*

a second computer system.".

5. Dependent claims 2-4, 6-15, 19-26 and 30-33 are allowable by virtue of their dependencies.

Conclusion

6. Any inquiry concerning this communication or earlier communications from examiner should be directed to Ronald Baum, whose telephone number is (571) 272-3861, and whose unofficial Fax number is (571) 273-3861 and unofficial email is Ronald.baum@uspto.gov. The examiner can normally be reached Monday through Thursday from 8:00 AM to 5:30 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kristine Kincaid, can be reached at (571) 272-4063. The Fax number for the organization where this application is assigned is **571-273-8300**.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. For more information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Ronald Baum

Patent Examiner

/R. B./

Examiner, Art Unit 2139

Kristine Kincaid

Kristine Kincaid

Supervisory Patent Examiner

AU 2139